IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF DELAWARE

IN RE GOOGLE INC. COOKIE PLACEMENT CONSUMER PRIVACY LITIGATION	)	C.A. No. 12-MD-2358 (SLR)
This Document Relates to: **All Actions**	)	

REPLY BRIEF IN SUPPORT OF DEFENDANT POINTROLL, INC.'S MOTION TO DISMISS

Alan Charles Raul
Edward R. McNicholas
SIDLEY AUSTIN LLP
1501 K Street, N.W.
Washington, D.C. 20005
Telephone: (202) 736-8000
Facsimile: (202) 736-8711
araul@sidley.com
emcnicho@sidley.com

Attorneys for Defendant PointRoll, Inc.

Susan M. Coletti (#4690)
FISH & RICHARDSON P.C.
222 Delaware Avenue, 17th Floor
P.O. Box 1114
Wilmington, DE 19899-1114
Telephone: (302) 652-5070
coletti@fr.com

Attorneys for Defendant PointRoll, Inc.

April 26, 2013

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

OTHER AUTHORITIES

Not only does Plaintiffs' consolidated amended complaint ("CAC") fail to allege sufficient facts to state any claim against PointRoll under the Wiretap, Stored Communications ("SCA"), and Computer Fraud and Abuse ("CFAA") Acts, it fails to allege nearly any relevant facts against PointRoll at all. Their brief makes spurious legal arguments routinely rejected by other courts. Even counsel for co-Plaintiffs acknowledged the federal claims "are inapplicable."[1] The criminal wiretapping, intrusion and hacking statutes invoked by Plaintiffs simply do not apply to cookies. Moreover, Plaintiffs have not carried their constitutional burden of establishing injury-in-fact. They offer no factual allegation or declaration that any Plaintiff actually had a PointRoll cookie in his or her Safari browser's cookie cache; that the content of any Plaintiffs' actual communication or personally identifiable information ("PII") was intercepted or accessed; or that any Plaintiff suffered any legally cognizable injury. Plaintiffs' arguments do nothing to overcome the numerous precedents rejecting liability for placing cookies (even supposedly unwanted ones) under the federal statutes at issue. Given the absence of relevant factual allegations against PointRoll, and the consistent failure of these types of federal claims, the CAC fails and should be dismissed with prejudice.

I. Plaintiffs Fail To Allege Injury-In-Fact To Confer Article III Standing

Despite its length, the CAC alleges very few facts against PointRoll. Plaintiffs fail to plead facts supporting the statutory claims or any injury-in-fact from PointRoll's alleged activities, undermining standing. They plead only "highly speculative" concerns and assumptions "set[ting] forth no specific facts" detailing any actual injury-in-fact, and thus do not have standing. *See Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013) (rejecting standing for alleged Constitutional violation because speculative, non-particularized allegations did not

[1] Motion by Daniel Mazzone and Michelle Kuswanto for Intervention as Plaintiffs at 14-15, *In re Google Inc. Cookie Placement Consumer Privacy Litigation*, No. 1:12-md-02358-SLR (D. Del. Jan. 16, 2013) (D.I. 64).

establish injury-in-fact).[2] Even if statutory claims could suffice for standing in the absence of concrete injury, plaintiffs failed to allege plausible statutory claims. Notably, they fail to allege the following essential facts: that any named Plaintiff actually has a PointRoll cookie on his computer; that any named Plaintiff's actual communications were intercepted; or that PointRoll acquired any actual information about specific websites actually visited by any named Plaintiff.

Plaintiffs wrongly argue they only have to plead "an identifiable trifle" of harm.[3] As *Twombly, Iqbal*, and their progeny make clear, Plaintiffs must do more than assert they experienced a trifle of alleged, non-specific harm as argued in their Opposition. D.I. 80 at 3. Claims must cross "the line from conceivable to plausible." *Bell Atl. Corp v. Twombly*, 550 U.S. 544, 547 (2007). Plaintiffs, however, rely almost exclusively on the disparaged dicta in *U.S. v. SCRAP* to argue that literally *any* harm is sufficient to establish standing–essentially gutting current standing doctrine.[4] Nothing in their opposition helps Plaintiffs over even that low bar.

Although Plaintiffs allege that PII has value (CAC ¶¶49-67), they do not (and cannot) establish that PointRoll impaired, lessened, or otherwise damaged that value. Article III standing requires *injury* to plaintiffs. Plaintiffs allege harm only as "a legal conclusion couched as a factual allegation." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). Courts have denied standing even in the face of significantly more developed allegations. *See In re Google Android Consumer Privacy Litig.*, 2013 WL 1283236, at *4 (N.D. Cal. Mar. 26, 2013) ("[D]istrict courts

---

[2] Plaintiffs disparage PointRoll's standing argument because PointRoll demonstrates that the federal statutes invoked by Plaintiffs do not apply before arguing standing. However, this was precisely the approach adopted by the court in *In re Google, Inc. Privacy Policy Litigation*, 2012 WL 6738343, at *5-8 (N.D. Cal. Dec. 28, 2012). In any event, Plaintiffs have the burden to establish standing, and the Court is without jurisdiction to hear the case if Plaintiffs fail to prove it. *See Focus v. Allegheny Cnty. Ct. Com. Pl.*, 75 F.3d 834, 838 (3d Cir. 1996).

[3] D.I. 80 at 3-4 (citing *United States v. Students Challenging Reg. Agency Procedures ("SCRAP")*, 412 U.S. 669, 689 n. 14 (1973)).

[4] *See Lujan v. Nat'l Wildlife Fed'n*, 497 U.S. 871, 889 (1990) (SCRAP's "expansive expression of what would suffice for [standing under the Administrative Procedure Act] under its particular facts has never since been emulated by this Court . . . .").

have been reluctant to find standing based solely on a theory that the value of a plaintiff's PII has been diminished.")[citing cases]. As in that case, Plaintiffs here do not allege any facts suggesting that PointRoll "attempted to sell their personal information, that they would do so in the future, or that they were foreclosed from entering into a value for value transaction relating to their PII, as a result of the [defendant's] conduct." *Id.*

II. Plaintiffs Fail To Plead Statutory Violations That Satisfy Applicable Standards

Plaintiffs attempt to mask the insufficiency of their pleading by arguing from broad generalities rather than specific facts pled in the CAC. *See* D.I. 53. Lacking facts, Plaintiffs offer hypothetical inferences and inconsistent conclusions about PointRoll's cookies. CAC ¶¶ 139-145. Courts may draw "reasonable inference[s]," but must do so based upon *factual* allegations.[5]

The CAC acknowledges and concedes the basic structure of Internet advertising: visitors to a website where PointRoll serves ads receive ad content from PointRoll.[6] This admission, importantly, renders Plaintiffs' legal conclusions implausible because it means that PointRoll is necessarily a party to the user's communication request in order to be able to serve the advertisement on that page.[7] Indeed, PointRoll serves an advertisement to the user regardless of any setting or placement of cookies. Cookies simply record information that is already available

---

[5] Plaintiffs must plead "sufficient factual matter . . . to state a claim to relief that is plausible on its face." *Iqbal*, 556 U.S. at 678. *See also, e.g., White v. Hon Co.*, 2013 WL 1386201, at *2 (3d Cir. Apr. 5, 2013) ("[Plaintiffs] may not attempt to use discovery as a fishing expedition... to seek out the facts necessary to establish a legally adequate complaint.") (citing *Ranke v. Sanofi–Synthelabo Inc.*, 436 F.3d 197, 204 (3d Cir. 2006)); *Burtch v. Miliberg Factors, Inc.*, 662 F.3d 212, 226 (3d Cir. 2011) (affirming dismissal of a complaint where allegations regarding key facts were pleaded as unknown or without records); *Manuel v. Mears*, 2012 WL 4863061, at *2 n.2 (D. Del. Oct. 11, 2012).

[6] Plaintiffs concede that users' computers initiate communications with PointRoll when their browser requests website content and triggers a GET request sent by the browser to PointRoll for ad content. CAC ¶¶ 41, 129. The GET request communicates information regarding the browser's online activities to PointRoll directly, and has nothing to do with PointRoll's alleged, subsequent use of cookies. Plaintiffs' GET submissions are "intended for" websites, and the browsers or websites intentionally direct PointRoll to serve ads to be displayed on those sites.

[7] As Plaintiffs concede, "the PointRoll server responds to the GET request." D.I. 80 at 2.

to the party serving the advertisement – PointRoll – (such as the user's IP address and the address of the website on which the ad is served) because it served the ad to the user on the page the user visited. Plaintiffs' allegations do not (and cannot) refute this basic reality of the Internet: cookies do not make such communications possible or extract information from the user, they merely allow parties serving advertisements to record information that such party would know whether it sets a cookie or not.[8]

III. Plaintiffs' Wiretap Allegations Should Be Dismissed

Plaintiffs fail to rebut any of PointRoll's reasons for dismissing the Wiretap Act counts. The Wiretap Act simply does not cover the use of cookies or the collection of transactional information through such mechanisms. *E.g., In re iPhone Application Litig.,* 844 F. Supp. 2d 1040, 1061-62 (N.D. Cal. 2012); *In re Facebook Privacy Litig.,* 791 F. Supp. 2d 705, 709-713 (N.D. Cal. 2011); *In re DoubleClick Inc. Privacy Litig.,* 154 F. Supp. 2d 497 (S.D.N.Y. 2001); *Chance v. Avenue A*, *Inc.*, 165 F. Supp. 2d 1153, 1162 (W.D. Wash. 2001).

A. PointRoll Is A Party To Any Communication Through Which It Serves Ads

PointRoll is necessarily a party to any communication through which it serves advertisements. Plaintiffs effectively concede this point (CAC ¶41, 129), and certainly cannot dispute it. *See, e.g., In re DoubleClick Inc.,* 154 F. Supp. 2d at 511.[9]

---

[8] In recent testimony to Congress, for example, the Digital Advertising Alliance explained that where consumers opt out of cookies "they will still receive advertising … [and] web viewing data may still be collected for narrow purposes including operational and system management purposes, fraud prevention and security, content delivery …." *Hearing on A Status Update on the Development of Voluntary Do-Not-Track Standards Before the S. Comm. on Commerce, Sci. & Transp.*, at 4 (Apr. 24, 2013)(statement of Luigi Mastria, Managing Director, Digital Advertising Alliance), *available at* http://www.aboutads.info/resource/4.23.13_DAA_Testimony.pdf.

[9] Even if one adopts Plaintiffs' position that consent is an affirmative defense, the Wiretap Act claims are still properly dismissed because the presence of consent appears on the face of the pleadings. *See Day v. Moscow*, 955 F.2d 807, 811 (2d Cir. 1992) ("[W]hen all relevant facts are

There can be no plausible debate about whether the websites on which PointRoll served ads authorized PointRoll to deliver ad content by communicating with users' browsers. CAC ¶¶ 41, 129. Plaintiffs do not dispute that websites allocate space for ads served by PointRoll. As in *DoubleClick* "it [is] implausible to infer that the Web sites have not authorized [the ad serving company's] access." *In re DoubleClick Inc.*, 154 F. Supp. 2d at 510. Thus, PointRoll was an authorized party to the website's communication with users, and it necessarily knew on which websites it was serving ads and to which user IP addresses it was delivering those ads. Accordingly, it could not "intercept" any of this information in either a legal or colloquial sense. It simply needs and uses this information – regardless of cookies – to serve ads on particular websites to particular IP addresses (of users seeking to view those websites).

Plaintiffs newly argue that Safari browsers were "specifically configured to ***prohibit*** PointRoll from becoming a party" to the communications (D.I. 80 at 10), but this argument is baseless. So long as websites authorize PointRoll to serve ads to users visiting those websites, PointRoll will be a party to those communications. Plaintiffs cannot change the structure of the Internet through specious briefing. Nothing about Safari's default cookie settings - or any facts alleged by Plaintiffs - prevents or inhibits websites from displaying advertisements, or limits information communicated by the browser to the entity serving the ads on those websites.[10]

B. **Plaintiffs Fail To Plead Interception Of "Content"**

Plaintiffs' argument that some URLs could conceivably reflect the content of electronic

---

shown by the court's own records, of which the court takes notice, the [affirmative] defense may be upheld on a Rule 12(b)(6) motion without requiring an answer.").

[10] Plaintiffs' novel suggestion of some "affiliation with Apple" (appearing for the first time in their brief and without support in the CAC), is also self-defeating. It would undermine their argument for Plaintiffs to imply that Apple was somehow working with PointRoll. In any event, Plaintiffs do not (and cannot) allege that Apple imposed any of its cookie settings on PointRoll, directly signaled anything to PointRoll, or had any particular point of view regarding PointRoll's ad effectiveness cookies.

communications does nothing to overcome the absence of any facts pleaded in the CAC to support the inference that PointRoll actually "intercepted" any such content of actual communications of any named Plaintiff. D.I. 53 at 5-6. The CAC lacks any factual allegations about what content PointRoll's cookies supposedly collected or how.[11] Plaintiffs do not allege how they interacted with any ad served by PointRoll, or what information—content or otherwise—PointRoll received as a result. Plaintiffs are likewise uniquely positioned to identify their own historical browsing activites but failed to do so, proffering instead only self-serving legal conclusions. This is not merely an omission or inadequacy in briefing; they neglect these points because such information does not exist, and the information that does exist is undoubtedly not helpful to their claims.[12]

C. Plaintiffs Cannot Point To Any "Device" PointRoll Used

Plaintiffs similarly cannot save a Wiretap claim by imagining that software code constitutes a "device." CAC ¶201. While Plaintiffs argue that "[n]o court has ever found that servers, browsers, cookies, or any schemes using them . . . are not 'devices'" (D.I. 80 at 13), the real point is that Plaintiffs have cited no case for the proposition that cookies, browsers, servers and schemes *are* "devices" for purposes of the Wiretap Act. Accordingly, they offer the Court no

[11] Even if one assumes PointRoll acquired URLs as a result of browsers' direct communications with PointRoll's server, Plaintiffs do not provide any plausible allegation that PointRoll obtained anything beyond the domain or IP of a website on which it served ads. *See e.g., U.S. v. Forrester*, 495 F.3d 1041, 1048-49 (9th Cir. 2007) (IP addresses do not necesarily reveal more about the contents of a communication than does a phone number). According to the Mayer article, URLs stored in the PointRoll cookies were for domain names, not file names, and would thus be unlikely to reveal content. Jonathan Mayer, *Safari Trackers*, Web Policy Blog (Feb. 17, 2012), http://webpolicy.org/2012/02/17/safari-trackers/. Plaintiffs have not pled that PointRoll intercepted any particular content contained in an actual (as opposed to hypothetical) URL.

[12] Plaintiffs allege that a GET request could contain "substantive content of an intercepted communication," but fail to identify any examples of how this involved PointRoll or any instance where any of their data was intercepted beyond a general reference to hypothetical websites with no apparent tie to PointRoll's ad serving activities. CAC ¶207. To the extent that the hypothetical URL was intended to denote a page on which PointRoll served an ad, PointRoll would certainly already know that information.

legal support (or plausible factual allegation) to hold that PointRoll used any "device" in connection with any putative "interception" of any "content" of any actual communication.

IV. Plaintiffs' Response Demonstrates The Insufficiency Of Their SCA Claims

Co-Plaintiffs hit the nail on the head by explaining that "the SCA, which is construed narrowly, does not apply to [Defendants'] alleged conduct. In brief, this is because computers and mobile devices are not 'facilities' under the SCA and because, even if those devices were 'facilities,' the MDL Plaintiffs cannot allege that [Defendants] obtained access to a communication that was in 'electronic storage'." D.I. 64 at 14-15. Rarely does a Defendant agree so completely with a brief submitted by the Plaintiffs' counsel: the SCA does not apply to the setting of cookies or other downloaded data. *See e.g. Garcia v. City of Laredo*, 702 F.3d 788 (5th Cir. 2012); *In re iPhone Litig.,* 844 F. Supp. 2d at 1057-58; *Thompson v. Ross,* 2010 WL 3896533, at *5 (W.D. Pa. Sept. 30. 2010); *In re DoubleClick, Inc.*, 154 F. Supp. 2d at 512; *In re Toys R Us, Inc., Privacy Litig.*, 2001 WL 34517252, at *3-4 (N.D. Cal. Oct. 9, 2001).

Plaintiffs nonetheless attempt to characterize a browser's cookie cache, or user computers upon which they are stored, as "facilities through which an electronic communication service is provided." CAC ¶¶ 216-18. This is entirely unsupported. Electronic communication service ("ECS") providers include internet service providers and telecommunications providers. Plaintiffs do not and cannot credibly allege that PointRoll or the Safari software is an ECS that provides the internet service through which browsers communicate, and this failure is fatal to their SCA claim. *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 524 (N.D. Ill. 2011).

Plaintiffs should not be allowed to implausibly assert that internet service is somehow provided through browser-managed files or user computers, though neither PointRoll nor Safari are ECS providers. D.I. 80 at 15. Components that only enable such data transport, like

computers and browser software, are not "facilities."[13]

Plaintiffs attempt to point to *Council on American-Islamic Relations Action Network, Inc. v. Gaubatz*, 793 F. Supp. 2d 311 (D.D.C. 2011), to argue that Congress intended "facilities" to include physical equipment used to enable electronic communications. D.I. 80 at 15. They ignore, however, that when evaluating a factually analogous scenario the *Gaubatz* court held that the SCA "clearly is not triggered when a defendant merely accesses a physical client-side computer and limits his access to documents stored on the computer's local hard drive or other physical media." 793 F. Supp. 2d at 335 (citing *United States v. Steiger*, 318 F.3d 1039, 1049 (11th Cir. 2003)).[14] Likewise, Plaintiffs' reliance on *Cousineau v. Microsoft Corp.*, No. C11-1438-JCC (W.D. Wash. June 22, 2012), is inapposite. The *Cousineau* court stated, with hardly any analysis, that a mobile phone could be a facility where a provider used the phone as part of its equipment to provide the service. *Id.* at 12. None of that is relevant here. Plaintiffs do not allege that any ECS provider used Plaintiffs' phones to provide the ECS. In any event, *Cousineau* is a distinct outlier insufficient to overcome the weight of appellate and district cases holding that personal computers are *not* "facilities."[15]

---

[13] *See, e.g., Garcia,* 702 F.3d at 792 ("facilities" do not include computers that enable the use of an ECS, but that are operated by an ECS); *Shefts v. Petrakis,* 2013 WL 489610*,* at *4 (C.D. Ill. Feb. 8, 2013)*; In re Michaels Stores*, 830 F. Supp. 2d at 524 ("Plaintiffs do not allege that Michaels provides the internet or phone service is . . .[This] is fatal to Plaintiffs' claim that Michaels provides [ECS] under the SCA."); *Freedom Banc Mortg. Servs., Inc. v. O'Harra*, 2012 WL 3862209, at *9 (S.D. Ohio Sept. 5, 2012) ('facilities' "are not computers that enable the use of an [ECS], but instead are facilities that are operated by [ECS] providers."). *See also Crowley v. Cybersource Corp.*, 166 F. Supp. 2d 1263, 1271 (N.D. Cal. 2001) (plaintiffs' argument "that computers of users of [ECS], as opposed to providers of [ECS], are considered facilities through which such service is provided" was "destined for failure.").

[14] The *Gaubatz* Court distinguished the facts at hand by emphasizing that the defendant allegedly accessed more than files stored on an office computer's local hard drives, by accessing Plaintiffs' computer servers, networks, or systems through which Plaintiff arguably provided ECS. 793 F. Supp. 2d at 335.

[15] *See Garcia,* 702 F.3d 788 (reviewing legislative history and prior decisions and concluding cell phones are not "facilities" under the SCA); *Steiger*, 318 F.3d at 1049 (SCA does not apply to

Further, none of Plaintiffs' suggestions overcome their failure to show that any data allegedly retained by and accessed from PointRoll's cookies was in "electronic storage." *Garcia*, 702 F.3d at 793 ("Electronic storage" encompasses only information stored by an ECS provider). Information in cookies falls outside of the narrow statutory definition of "electronic storage."[16]

V. Plaintiffs Fail To Plead A Viable CFAA Claim

Plaintiffs failed to allege the types of "damages" or "loss" that constitute redressable injury under the CFAA. Instead they attempt to bypass existing law and allege injuries not recognized by the CFAA.[17] Plaintiffs suggest that PointRoll's use of cookies "impaired" the Safari browser "default system setting," but do not allege facts to support such an inference. Nothing supports the suggestion that blocking cookies would prevent ads.[18] Plaintiffs simply have not and cannot support their conclusion that placing cookies violates the CFAA.[19] Further,

---

"hacking into personal computers to retrieve information stored therein"); *In re DoubleClick,* 154 F. Supp. 2d at 512 (the Senate Report on SCA "deals only with facilities operated by [ECS]…. It makes no mention of individual users' computers."); *In re iPhone Litig.,* 844 F. Supp. 2d at 1057 (individual's computer, laptop, or mobile devices is not a 'facility through which an [ECS] is provided'); *Shefts*, 2013 WL 489610 at *3 (text messages stored on a blackberry or the Access2Go server were not in a "facility" because neither provided the text messaging service that transmitted the stored messages); *Navarro v. Verizon Wireless, LLC,* 2013 WL 275977, at *3 (E.D. La. Jan. 24, 2013).

[16] *See Shefts*, 2013 WL 489610 at *3 (communications on a device not stored *by* the ECS are not in "electronic storage"); *Bailey v. Bailey*, 2008 WL 324156, at *6 (E.D. Mich. Feb. 6, 2008) (SCA "protection does not extend to [data] stored only on Plaintiff's personal computer"); *Thompson*, 2010 WL 3896533 at *5 (messages stored on and later accessed from a user's personal computer are not in electronic storage.).

[17] Plaintiffs offer no response to the argument that, were their CFAA claims to stand, online advertising would conceivably be criminalized if a browser's setting were ignored or exceeded. This flies in the face of the concepts of jurisprudential lenity and restraint. *See, e.g., United States v. Nosal*, 676 F.3d 854, 860 (9th Cir. 2012); *CBS Corp. v. FCC*, 663 F.3d 122, 174 n.19 (3d Cir. 2011).

[18] As the Mayer article explains, PointRoll set cookies in a manner that was consistent with the exceptions that Apple built into the Safari default settings; nowhere does it suggest that cookies somehow changed the browser's code. Indeed, Safari's code included three means by which third-party domains could drop cookies. Mayer, *Safari Trackers*, *supra* note 12, at 6.

[19] *See, e.g.*, *In re iPhone Litig.*, 844 F. Supp. 2d at 1066 (citing cases); *Del Vecchio v. Amazon.com, Inc.*, 2012 WL 1997697, at *5 (W.D. Wash. June 1, 2012); *Bose v. Interclick, Inc.*,

Plaintiffs fail to address PointRoll's demonstration that Plaintiffs' CFAA allegations under 18 U.S.C. §§ 1030(a)(2)(c), (a)(5)(a)(i), and (a)(5)(a)(iii) warrant dismissal, effectively abandoning those claims. Instead, they now pursue a claim under 18 U.S.C. § 1030(a)(4).[20] D.I. 80 at 18-20. The CAC did not include this claim and it should not be considered. *Grayson v. Mayview State Hosp.*, 293 F.3d 103, 109 n. 9 (3d Cir. 2002) (plaintiffs "should not be able effectively to amend a complaint through any document short of an amended pleading").[21]

Regardless, the newly introduced claim fails because the only "value" allegedly obtained by PointRoll was use of Plaintiffs' computers and personal information, which is insufficient to cause a loss that would support an action under 18 U.S.C. § 1030(a)(4). *Del Vecchio*, 2012 U.S. Dist. LEXIS 76536, at *10-13; *In re iPhone Litig.*, 844 F. Supp. 2d at 1068 ("[C]ourts have tended to reject the contention that [losses relating to] personal information . . . constitutes economic damages under the CFAA."). Further, Plaintiffs nowhere plead facts suggesting PointRoll acted with the necessary intent to defraud.[22] Plaintiffs' new claim should be rejected as swiftly as Plaintiffs themselves abandoned their other CFAA claims. *See, e.g., P.C. Yonkers, Inc. v. Celebrations the Party & Seasonal Superstore, LLC*, 428 F.3d 504, 509-10 (3d Cir. 2005) (rejecting CFAA claim under § 1030(a)(4) where plaintiffs could not show intent to defraud).

2011 WL 4343517, at *6-7 (S.D.N.Y. Aug. 17, 2011); *LaCourt v. Specific Media, Inc.,* 2011 WL 1661532, at *4-5 (C.D. Cal. Apr. 28, 2011); *Chance*, 165 F. Supp. 2d at 1156; *In re DoubleClick Inc.*, 154 F. Supp. 2d at 503-04.

[20] This provision permits a claim against anyone who "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and … furthers the intended fraud and obtains anything of value."

[21] *See also Aldinger v. Spectrum Control, Inc.*, 207 F. App'x 177, 180 n. 1 (3d Cir. 2006) (refused to address issues introduced in briefing and not pleaded in the complaint).

[22] Plaintiffs' speculation about PointRoll's intent still does not show that PointRoll "(1) accessed a 'protected computer,' (2) without authorization or exceeding such authorization that was granted, (3) 'knowingly' and with 'intent to defraud,' and thereby (4) 'further[ed] the intended fraud and obtain[ed] anything of value,' causing (5) a loss to one or more persons during any one-year period aggregating at least $5,000 in value." *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1132 (9th Cir. 2009).

Respectfully submitted,

Dated: April 26, 2013

By: /s/ *Susan M. Coletti*

Alan Charles Raul
Edward R. McNicholas
SIDLEY AUSTIN LLP
1501 K Street, N.W.
Washington, D.C. 20005
Telephone: (202) 736-8000
Facsimile: (202) 736-8711
araul@sidley.com
emcnicho@sidley.com

Attorneys for Defendant PointRoll, Inc.

Susan M. Coletti (#4690)
FISH & RICHARDSON P.C.
222 Delaware Avenue, 17th Floor
P.O. Box 1114
Wilmington, DE 19899-1114
Telephone: (302) 652-5070
coletti@fr.com

Attorneys for Defendant PointRoll, Inc.

CERTIFICATE OF SERVICE

I hereby certify that on April 26, 2013, I electronically filed the foregoing with the Clerk of Court for the United States District Court for the District of Delaware by using the CM/ECF system. I certify that for all participants in the case that are registered CM/ECF users, service will be accomplished via the CM/ECF system:

/s/ Susan M. Coletti
Susan M. Coletti